

# Machine learning-based anomaly detection for smart home networks under adversarial attack

Juli Rejito<sup>1</sup>, Deris Stiawan<sup>2</sup>, Ahmed Alshaflut<sup>3</sup>, Rahmat Budiarto<sup>4</sup>

<sup>1</sup>Department of Computer Science, Faculty of Mathematics and Science, Universitas Padjadjaran, Indonesia

<sup>2</sup>COMNETS RG, Faculty of Computer Science, Universitas Sriwijaya, Palembang, Indonesia

<sup>3</sup>Department of Information Technology, College of Computing and Information, Al-Baha University, Albaha, Saudi Arabia

<sup>4</sup>Department of Computer Science, College of Computing and Information, Al-Baha University, Albaha, Saudi Arabia

## Article Info

### Article history:

Received Nov 3, 2023

Revised Jan 3, 2024

Accepted Feb 17, 2024

### Keywords:

Adversarial attack

Generative adversarial network

Machine learning

Multi layer perceptron

Smart network

## ABSTRACT

As smart home networks become more widespread and complex, they are capable of providing users with a wide range of applications and services. At the same time, the networks are also vulnerable to attack from malicious adversaries who can take advantage of the weaknesses in the network's devices and protocols. Detection of anomalies is an effective way to identify and mitigate these attacks; however, it requires a high degree of accuracy and reliability. This paper proposes an anomaly detection method based on machine learning (ML) that can provide a robust and reliable solution for the detection of anomalies in smart home networks under adversarial attack. The proposed method uses network traffic data of the UNSW-NB15 and IoT-23 datasets to extract relevant features and trains a supervised classifier to differentiate between normal and abnormal behaviors. To assess the performance and reliability of the proposed method, four types of adversarial attack methods: evasion, poisoning, exploration, and exploitation are implemented. The results of extensive experiments demonstrate that the proposed method is highly accurate and reliable in detecting anomalies, as well as being resilient to a variety of types of attacks with average accuracy of 97.5% and recall of 96%.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



## Corresponding Author:

Juli Rejito

Department of Informatics, Faculty of Mathematics and Science, Universitas Padjadjaran

Jl. Raya Bandung Sumedang KM.21, Hegarmanah, Jatinangor, Jawa Barat 45363, Indonesia

Email: juli.rejito@unpad.ac.id

## 1. INTRODUCTION

As smart home networks become more widespread and intricate, they provide users with access to a wide range of applications and services, ranging from smart lighting and heating to security [1]. These networks are composed of a variety of devices, including sensor, actuator, camera, and smart appliance sensors, that interact with one another and external servers through either wireless or wired communication protocols [2]. These devices and protocols, however, often have low levels of security and are susceptible to a variety of attacks from malicious adversaries. These attacks may include denial of service (DOS) attacks to disrupt network functionality, phishing attacks to create a false identity for a legitimate device or user, listening in on conversations to acquire sensitive information, and tampering attacks to modify the device's status or commands [3]–[6]. The consequences of these attacks can range from privacy violations to property damage and even physical harm.

To identify and prevent attacks on smart home networks, anomaly detection is a useful method. It observes the network behavior and spots any abnormal changes that suggest malicious actions. The detection can happen at various levels of detail, such as device-level, network-level, or application-level [7]; it can also use

different kinds of data sources, such as device states, network traffic, user feedback, or environmental factors [8], [9]. Furthermore, anomaly detection can provide prompt warnings and reactions to the users or network administrators, and assist in securing the smart home networks from potential threats [10].

Nevertheless, anomaly detection in smart home networks faces several challenges that require novel solutions [1]. One of the main challenges is the presence of adversarial attacks that can manipulate the network data or models to evade or mislead the anomaly detection systems [11]. An adversarial attack occurs when an adversarial example is fed as an input to a machine learning model. An adversarial example is an instance of the input in which some feature has been intentionally perturbed with the intention of confusing a machine learning model to produce a wrong prediction. Adversarial attacks can be launched at different stages of the anomaly detection process, such as data collection, feature extraction, model training, or model inference. Adversarial attacks can also have different objectives and strategies, such as reducing the detection accuracy, increasing the false alarm rate, or causing specific misclassifications, which in turn can pose serious threats to the reliability and robustness of the anomaly detection systems in smart home networks.

Many research works attempt to address the issues of adversarial attacks on smart home network have been proposed. A popular way to find anomalies in smart home networks is to rely on network traffic data as the primary information source. Network traffic data can record the exchanges and connections between the network devices and servers, and show the network activity and quality. Network traffic data can be examined using different methods, such as statistical methods, rule-based methods, clustering methods, or machine learning methods.

As an example, Wang, *et al.* [12] proposed a statistical method that uses entropy and correlation coefficient to identify abnormal patterns in smart home networks. Kalnoor and Gowrishankar [13] introduced a statistical method that uses Markov chains and hypothesis testing to identify abnormal patterns in IoT networks. Statistical methods are simple and efficient, but they may suffer from low accuracy and high false alarm rate, especially when the network traffic data is noisy or non-stationary. Usman, Muthukkumarasamy and Wu [14] suggested a rule-based method that uses fuzzy logic to identify abnormal patterns in smart home networks. Graf, *et al.* [15] proposed a rule-based method that uses decision trees to identify abnormal patterns in smart home networks. Rule-based methods are easy to apply and understand, but they may lack adaptability and scalability, especially when the network traffic data is dynamic or heterogeneous. Gadal, *et al.* [16] and Stiawan, *et al.* [17] suggested a clustering method that uses K-Means to identify abnormal patterns in smart home networks. Li, *et al.* [18] suggested a clustering method that uses density-based spatial clustering of applications with noise (DBSCAN) to identify abnormal patterns in smart home networks. Clustering methods are flexible and robust, but they may require high computational complexity and sensitivity to parameters, especially when the network traffic data is high-dimensional or sparse. Using supervised or semi-supervised learning techniques, machine learning methods train classifiers that can separate normal and abnormal behaviors in network traffic data [19]. For instance, Nanthiya, *et al.* [20] proposed a machine learning method that uses support vector machines (SVM) to identify anomalies in smart home networks. Similarly, Bokka and Sadasivam [21] and Latif *et al.* [22] proposed a machine learning method that uses deep neural networks (DNN) to identify anomalies in smart home networks. Machine learning methods are effective and precise, but they may need high data and model resources and have low explainability, especially when the network traffic data is skewed or complicated.

This paper proposes a machine learning-based anomaly detection method for smart home networks under adversarial attack. The proposed method leverages the network traffic data and extracts relevant features to train a supervised classifier that can distinguish between normal and anomalous behaviors. Various adversarial attack scenarios are also designed and implemented to evaluate the performance and robustness of the proposed method. Then, extensive experiments on real-world smart home network datasets are conducted and the results are compared with several baseline methods.

The main contributions of this paper are as follows,

- A novel machine learning-based anomaly detection method for smart home networks that can handle both benign and malicious anomalies.
- Design and implementation of various adversarial attack scenarios that target different stages and objectives of the anomaly detection process.

The rest of this paper is organized as follows: Section 2 describes the proposed methodology of our machine learning-based anomaly detection method. Section 3 presents and analyzes the experimental set up and results of our method under different adversarial attack scenarios. Section 4 concludes the paper and provides an outlook on the future work.

## 2. METHOD

This section describes the proposed methodology of the machine learning-based anomaly detection method for smart home networks under adversarial attack. The proposed methodology consists of four main

steps: data collection and preprocessing, feature extraction and selection, model training and testing, and evaluation. Figure 1 shows the overview of the proposed methodology.

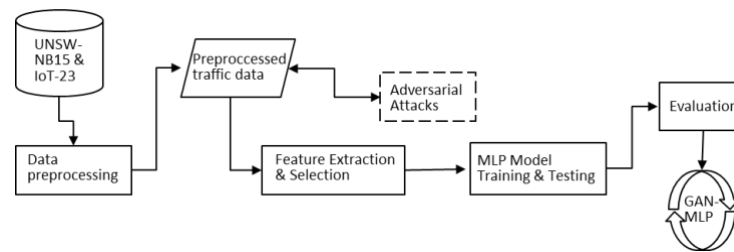


Figure 1. Steps in the proposed GAN-MLP

## 2.1. Data preprocessing

The first thing to do in the proposed method is to get and clean up the data of network traffic from smart home networks. Two real-world datasets of smart home network traffic, i.e. the UNSW-NB15 [23] and the IoT-23 datasets [24]. The UNSW-NB15 dataset has 9 kinds of good and bad network traffic situations from 49 IoT devices, like sensors, actuators, or routers. The IoT-23 dataset has 20 kinds of good and bad network traffic situations from 23 IoT devices, like cameras, thermostats, or smart plugs. Both datasets give us a lot of information about the network packets, like where the packets come from and go to, what ports and protocols are used, how big the packet is, or when the attacks happen. The two datasets represent smart home network traffic. The preprocessing of the network traffic data involves the following steps,

- Filter out the irrelevant or redundant packets that do not belong to the smart home network devices or servers.
- Aggregate the packets into flows based on the five-tuple (source IP, destination IP, source port, destination port, protocol) and a time window of 10 seconds.
- Label each flow as normal or anomalous based on the ground truth provided by the datasets. Then, assign each anomalous flow a specific type of anomaly based on the attack scenario, such as denial-of-service, spoofing, eavesdropping, or tampering.
- Normalize the numerical features of each flow using min-max scaling to avoid feature scaling issues.

## 2.2. Feature extraction and selection

The method's second step is to extract and select relevant features from the network traffic data that can represent the normal and abnormal behaviors of the smart home network devices. We have two kinds of features: basic and advanced. Basic features come from the network packets or flows directly, such as source and destination IP addresses, port numbers, protocols, payload sizes, or inter-arrival times. Advanced features are calculated using statistical or machine learning methods on the basic features, i.e.: principal component analysis (PCA). For each flow, 38 basic features and 18 advanced features are extracted in total. Then feature selection method is applied to simplify and lower the dimensionality of the feature space. A wrapper-based feature selection method that uses a machine learning classifier is deployed as a black box to assess the importance and relevance of each feature. We use recursive feature elimination (RFE) algorithm to gradually eliminate the least important features until we reach a desired number of features, and then choose 18 features as the best number based on the balance between accuracy and efficiency. The steps in recursive feature elimination (RFE) method are,

- Rank the importance of all features using the chosen RFE machine learning algorithm.
- Eliminate the least important feature.
- Build a model using the remaining features.
- Repeat steps 1-3 until the desired number of features is reached.

## 2.3. Model training and testing

The third step is to create and train a machine learning classifier that can identify normal and abnormal behaviors in smart home networks. A supervised learning technique that needs labeled data for training and testing is applied, and a multi-class classification technique that can generate multi-class decisions (normal or various kinds of anomalies) for each flow is used. The machine learning classifier is a multi layer perceptron (MLP). The MLP is an artificial neural network that has multiple layers of neurons that can learn complex and non-linear patterns from high-dimensional data.

Having done preliminary experiments, the best MLP has three hidden layers with 64 neurons each and a rectified linear unit (ReLU) activation function. The output layer has a softmax activation function that gives the class probabilities for each flow. The error between the true class labels and the predicted class probabilities is calculated by the categorical cross-entropy loss function. The weights of the MLP are updated by the Adam optimizer using gradient descent. The batch size is 128 and the epoch size is 10 for training. 80% of the network traffic data is used for training and 20% for testing. Stratified sampling is applied to make sure each class is equally represented in both sets. Two adversarial defense techniques are used to make the MLP more resilient to adversarial attacks. The first technique is adversarial training, which adds adversarial examples created by different attack methods to the training set. The second technique is distillation, which lowers the sensitivity of the MLP to adversarial perturbations by using parameters.

## 2.4. Evaluation metrics and criteria

To assess the effectiveness and resilience of the proposed anomaly detection method, we perform the final step of the proposed method. The accuracy and recall metrics are considered to evaluate the proposed method on 20% of the network traffic data as the testing data. Accuracy indicates how well the proposed method can distinguish between normal and anomalous flows. Recall indicates how well the proposed method can identify each type of anomalous flows. Various adversarial attack scenarios that aim at different goals and phases of the anomaly detection process are also created and executed. The four types of adversarial attack methods, i.e.: evasion, poisoning, exploration is used. Each adversarial attack method is implemented using different techniques and parameters, i.e.: gradient-based, optimization-based, random-based, or query-based methods. The success rate and impact of each adversarial attack method on the anomaly detection method was measured. The proposed method is also compared with several baseline methods, i.e.: SVM, K-Means, and decision tree (DT) under different adversarial attack scenarios. The accuracy and recall formula are shown in (1) and (2), respectively.

$$Accuracy = \frac{True\ positives + True\ Negatives}{True\ positives + True\ negatives + False\ positives + False\ negatives} \quad (1)$$

$$Recall = \frac{True\ positives}{True\ positives + False\ negatives} \quad (2)$$

## 2.5. Generative adversarial network

Figure 2 illustrates the generative adversarial network (GAN) implementation [25], [26]. The generative model takes into account the data distribution and is trained to maximize the likelihood that the Discriminator will make a mistake. On the other hand, the Discriminator relies on a model that predicts the likelihood that the sample received is obtained from the training data rather than from the Generator. Besides the MLP, four classifiers, i.e.: SVM, K-Means, decision tree (entropy-based method) and machine learning-based classifier [27]. GANs are defined as minimax games, in which the Discriminator seeks to maximize its reward ( $V(D, G)$ ) and the Generator seeks to maximize the Discriminator's reward (or, in other words, maximise its loss). The loss function is represented mathematically by the formula in (3) and (4) [26]. Figure 3 shows the algorithm for implementing the GAN in this research work.

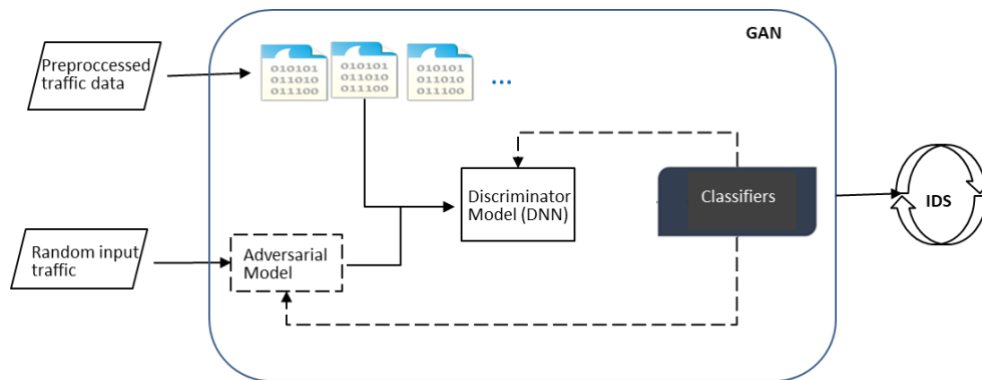


Figure 2. The generative adversarial network

$$\min_G \max_D V(D, G) \quad (3)$$

$$V(D, G) = \sum_{x \sim p_{data(x)}} [\log D(x)] + \sum_{x \sim p_{data(x)}} [(1 - \log D(G(z)))] \quad (4)$$

Where,

D = Discriminator

G = Generator

Pdata(x) = distribution of real data

P(z) = distribution of generator

x = sample from Pdata(x)

z = sample from P(z)

D(x) = Discriminator network

G(z) = Generator network

#### Algorithm GAN

While number of training iterations do

    While j < m steps do

        Input m sample data  $\{z^{(1)}, \dots, z^{(m)}\}$  from P(z) generator

        Input m sample data  $\{x^{(1)}, \dots, x^{(m)}\}$  from Pdata(x) dataset

        Update the discriminator using Equation (2)

    End while

    Input m sample data  $\{z^{(1)}, \dots, z^{(m)}\}$  from P(z) generator

    Update the discriminator using momentum and  $\nabla = \sum_{i=1}^m [(1 - \log D(G(z^{(i)})))]$

End while

Figure 3. Algorithm GAN

### 3. EXPERIMENT SET UP, RESULTS AND DISCUSSION

In this section, we present the experimental set up, results and discussion of the proposed anomaly detection system for smart home networks under adversarial attack. The performance and robustness of the proposed method are evaluated under different adversarial attack scenarios. Comparison with SVM, K-Means, decision tree (entropy-based) and machine learning-based classifiers are presented. The GAN is implemented using Pytorch on a highend PC with the hardware specification: 64 GB RAM, Intel Core I9-13900k CPU, and 500 GB SSD storage.

#### 3.1. Performance evaluation

We first evaluate the performance of the proposed detection system in terms of accuracy and recall on the testing data without any adversarial attacks. The accuracy measures the overall correctness of the proposed method in classifying normal and anomalous traffic flows. Recall measures the sensitivity of the proposed method in detecting each type of anomalous traffic flows. Table 1 shows the accuracy and recall values on the the UNSW-NB15 and IoT-23 datasets. As shown in Table 1, the proposed method achieves relatively high accuracy and recall on both datasets, indicating that the proposed method can effectively distinguish between normal and anomalous behaviors in smart home networks. The proposed method also achieves high recall for each type of anomaly, indicating that it can accurately detect different types of attacks in smart home networks.

Table 1. The accuracy and recall on the two datasets

Dataset	Accuracy	Recall				
		Normal	DoS	Spoof	Eavesdrop	tampering
UNSW-NB15	0.96	0.98	0.94	0.95	0.97	0.93
IoT-23	0.98	0.99	0.96	0.97	0.99	0.95

#### 3.2. Robustness evaluation

Next, the proposed method's robustness is evaluated under the following sub-scenarios: Evasion, poisoning, exploration, and exploit. Each sub-scenario includes four different types of attack: gradient-based attack, optimization-based attack, random-based attack, query-based attack. Then, each sub-scenario is tested using different methods and parameters, i.e.: accuracy and impact on UNSW-NB15 and IoT-23 datasets as shown in Table 2. The impact is the degradation of accuracy due to the adversarial attacks.

Table 2. Resilience evaluation result

Attack Type	Attack Technique	Accuracy		Impact	
		UNSW-NB15	IoT-23	UNSW-NB15	IoT-23
Evasion	Gradient-based	0.83	0.85	13%	13%
	Optimization-based	0.80	0.82	16%	16%
	Random-based	0.74	0.76	22%	22%
Poisoning	Gradient-based	0.79	0.81	17%	17%
	Optimization-based	0.77	0.79	19%	19%
	Random-based	0.73	0.73	23%	25%
Exploitation	Gradient-based	0.88	0.89	8%	9%
	Optimization-based	0.85	0.86	11%	13%
	Random-based	0.80	0.82	26%	26%
Exploration	Query-based	0.86	0.87	10%	11%

### 3.3. Comparison with other methods

Four methods: SVM, K-Means, decision tree (DT) and ML-based [27] are also implemented under the adversarial attack's situation for comparison. In addition, indirect comparisons with GAN-AE system, proposed by [28] that combined the GAN with auto encoder classifier. The accuracy of the proposed method under adversarial attacks is taken from the average of the results in Table 2. Table 3 shows the comparison results in term of average accuracy and recall.

Table 3. Comparison with other methods/systems

Method	Accuracy				Recall	
	No Adversary		Under Adversary		UNSW-NB15	IoT-23
	UNSW-NB15	IoT-23	UNSW-NB15	IoT-23		
SVM	0.96	0.97	0.75	0.78	0.95	0.96
K-Means	0.94	0.95	0.64	0.65	0.93	0.95
DT	0.94	0.96	0.70	0.76	0.94	0.95
ML [27]	0.97	0.98	0.70	0.74	0.98	0.98
GAN-AE [28]	N/A	0.95	N/A		N/A	0.94
Proposed system	<b>0.96</b>	<b>0.98</b>	<b>0.805</b>	<b>0.82</b>	<b>0.95</b>	<b>0.97</b>

### 3.4. Discussion

The proposed detection system was tested and found that it can detect anomalies in smart home networks with a good accuracy and sensitivity (recall), and can resist different kinds of adversarial attacks. The proposed method performs better than several existing methods, such as SVM, K-Means, decision tree (entropy-based) or machine learning [27] methods, in different adversarial attack situations. The proposed detection system uses the network traffic data and selects important features to train the MLP classifier that can tell apart normal and anomalous behaviors even under adversarial attack condition, because it uses some adversarial defense techniques, such as adversarial training and distillation, to improve the strength of the MLP classifier. Table 2 shows the worst impact of adversarial attacks on the proposed system is 26% accuracy degradation, which is acceptable [29]. Table 3 shows that the proposed system still performs well under adversarial attacks situation. Thus, the proposed method can offer a trustworthy and safe solution for smart home network anomaly detection. Furthermore, the proposed method can also support the researchers or practitioners to create and improve more efficient and strong anomaly detection system for smart home networks.

## 4. CONCLUSION

A machine learning-based anomaly detection system for smart home networks under adversarial attack has been proposed. The proposed method leveraged the network traffic data and extracted relevant features to train MLP classifier that could distinguish between normal and anomalous behaviors. The proposed system also applied adversarial training and distillation, to enhance the robustness of the MLP classifier. Experimental results showed the performance and robustness of the proposed method on two real-world smart home network data sets under different adversarial attack scenarios. We compared the proposed system with several baseline methods, such as SVM, K-Means, decision tree and ML-based methods. The results showed that the proposed system achieved high accuracy and recall in detecting anomalies in smart home networks on UNSW-NB15 and IoT23 datasets, and was resilient to different types of adversarial attacks. Some limitations are revealed after performing the experiments. The proposed method requires a large amount of labeled data for training and testing, which may not be available or feasible in real-world scenarios, and a fixed set of features that may not capture all the aspects of the network behavior or adapt to the changes in the network

environment. The use of MLP as the classifier may have high data and model requirements and low interpretability. Other limitation is that the proposed system is evaluated under specific adversarial attack scenarios that may not cover all the possible types or techniques of adversarial attacks. Some of the future directions included the use of semi-supervised learning techniques to reduce the dependency on labeled data, using more advanced feature extraction and selection techniques to capture more relevant and diverse features, using more sophisticated or explainable machine learning models or techniques for anomaly detection, and designing and implementing more realistic or comprehensive adversarial attack scenarios and defense techniques.

## REFERENCES




- [1] J. I. I. Araya and H. Rifà-Pous, "Anomaly-based cyberattacks detection for smart homes: A systematic literature review," *Internet of Things (Netherlands)*, vol. 22, 2023, doi: 10.1016/j.iot.2023.100792.
- [2] B. K. Sovacool and D. D. Furszyfer Del Rio, "Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies," *Renewable and Sustainable Energy Reviews*, vol. 120, 2020, doi: 10.1016/j.rser.2019.109663.
- [3] O. Taiwo and A. E. Ezugwu, "Internet of things-based intelligent smart home control system," *Security and Communication Networks*, vol. 2021, 2021, doi: 10.1155/2021/9928254.
- [4] T. A. A. Abdullah, W. Ali, S. Malebary, A. A. Ahmed Abdullah, T. A. Abdullah, and A. Ali Ahmed, "A review of cyber security challenges, attacks and solutions for internet of things based smart home," *IJCSNS International Journal of Computer Science and Network Security*, vol. 19, no. 9, pp. 139–146, 2019, [Online]. Available: <https://www.researchgate.net/publication/336717887>.
- [5] H. Chi, C. Fu, Q. Zeng, and X. Du, "Delay wreaks havoc on your smart home: delay-based automation interference attacks," *Proceedings - IEEE Symposium on Security and Privacy*, vol. 2022-May, pp. 285–302, 2022, doi: 10.1109/SP46214.2022.9833620.
- [6] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity*, vol. 4, no. 1, 2021, doi: 10.1186/s42400-021-00077-7.
- [7] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 1, pp. 303–336, 2014, doi: 10.1109/SURV.2013.052213.00046.
- [8] E. A. Abumera, H. A. Elzouka, and A. A. Saad, "Security framework for identifying threats in smart manufacturing systems using STRIDE approach," *2022 2nd International Conference on Consumer Electronics and Computer Engineering, ICCECE 2022*, pp. 605–612, 2022, doi: 10.1109/ICCECE54139.2022.9712770.
- [9] S. G. Abbas, S. Zahid, F. Hussain, G. A. Shah, and M. Husnain, "A threat modelling approach to analyze and mitigate botnet attacks in smart home use case," *Proceedings - 2020 IEEE 14th International Conference on Big Data Science and Engineering, BigDataSE 2020*, pp. 122–129, 2020, doi: 10.1109/BigDataSE50710.2020.00024.
- [10] R. Zhu, X. Wu, J. Sun, and Z. Li, "Research on smart home security threat modeling based on STRIDE-IAHP-BN," *Proceedings - 2021 20th International Symposium on Distributed Computing and Applications for Business Engineering and Science, DCABES 2021*, pp. 207–213, 2021, doi: 10.1109/DCABES52998.2021.00059.
- [11] J. Fu, L. Wang, J. Ke, K. Yang, and R. Yu, "GANAD: A GAN-based method for network anomaly detection," *World Wide Web*, vol. 26, no. 5, pp. 2727–2748, 2023, doi: 10.1007/s11280-023-01160-4.
- [12] Y. Sun, J. Yu, J. Tian, Z. Chen, W. Wang, and S. Zhang, "IoT-IE: an information-entropy-based approach to traffic anomaly detection in internet of things," *Security and Communication Networks*, vol. 2021, 2021, doi: 10.1155/2021/1828182.
- [13] G. Kalnoor and S. Gowrishankar, "A model for intrusion detection system using hidden Markov and variational Bayesian model for IoT based wireless sensor network," *International Journal of Information Technology (Singapore)*, vol. 14, no. 4, pp. 2021–2033, 2022, doi: 10.1007/s41870-021-00748-1.
- [14] M. Usman, V. Muthukkumarasamy, and X. W. Wu, "Mobile agent-based cross-layer anomaly detection in smart home sensor networks using fuzzy logic," *IEEE Transactions on Consumer Electronics*, vol. 61, no. 2, pp. 197–205, 2015, doi: 10.1109/TCE.2015.7150594.
- [15] J. Graf, K. Neubauer, S. Fischer, and R. Hackenberg, "Architecture of an intelligent intrusion detection system for smart home," *2020 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2020*, 2020, doi: 10.1109/PerComWorkshops48775.2020.9156168.
- [16] S. Gadal, R. Mokhtar, M. Abdelhaq, R. Alsaqour, E. S. Ali, and R. Saeed, "Machine learning-based anomaly detection using k-mean array and sequential minimal optimization," *Electronics (Switzerland)*, vol. 11, no. 14, 2022, doi: 10.3390/electronics11142158.
- [17] D. Stiawan *et al.*, "Ping flood attack pattern recognition using a K-means algorithm in an internet of things (IoT) network," *IEEE Access*, vol. 9, pp. 116475–116484, 2021, doi: 10.1109/ACCESS.2021.3105517.
- [18] X. Li, H. Ghodosi, C. Chen, M. Sankupellay, and I. Lee, "Improving network-based anomaly detection in smart home environment," *Sensors*, vol. 22, no. 15, 2022, doi: 10.3390/s22155626.
- [19] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, "Machine learning for anomaly detection: a systematic review," *IEEE Access*, vol. 9, pp. 78658–78700, 2021, doi: 10.1109/ACCESS.2021.3083060.
- [20] D. Nanthiya, P. Keerthika, S. B. Gopal, S. B. Kayalvizhi, T. Raja, and R. S. Priya, "SVM based DDoS attack detection in IoT using IoT-23 BotNet dataset," *3rd IEEE International Virtual Conference on Innovations in Power and Advanced Computing Technologies, i-PACT 2021*, 2021, doi: 10.1109/i-PACT52855.2021.9696569.
- [21] R. Bokka and T. Sadasivam, "Deep learning model for detection of attacks in the internet of things based smart home environment," *Advances in Intelligent Systems and Computing*, vol. 1245, pp. 725–735, 2021, doi: 10.1007/978-981-15-7234-0\_69.
- [22] S. Latif *et al.*, "Intrusion detection framework for the internet of things using a dense random neural network," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 9, pp. 6435–6444, 2022, doi: 10.1109/TH.2021.3130248.
- [23] N. Moustafa and J. Slay, "UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set)," *2015 Military Communications and Information Systems Conference, MilCIS 2015 - Proceedings*, 2015, doi: 10.1109/MilCIS.2015.7348942.
- [24] A. P. and M. J. Erquiaga, "IOT-23," 2023, [Online]. Available: <https://www.stratosphereips.org/datasets-iot23>.
- [25] I. J. Goodfellow *et al.*, "Generative adversarial nets," *Advances in Neural Information Processing Systems*, vol. 3, no. January, pp. 2672–2680, 2014, doi: 10.1007/978-3-658-40442-0\_9.






- [26] T. Schlegl, P. Seeböck, S. M. Waldstein, U. Schmidt-Erfurth, and G. Langs, "Unsupervised anomaly detection with generative adversarial networks to guide marker discovery," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10265 LNCS, no. 2, pp. 146–147, 2017, doi: 10.1007/978-3-319-59050-9\_12.
- [27] T. Li, Z. Hong, and L. Yu, "Machine learning-based intrusion detection for IoT devices in smart home," *IEEE International Conference on Control and Automation, ICCA*, vol. 2020-Octob, pp. 277–282, 2020, doi: 10.1109/ICCA51439.2020.9264406.
- [28] T. Zixu, K. S. K. Liyanage, and M. Gurusamy, "Generative adversarial network and auto encoder-based anomaly detection in distributed IoT networks," *2020 IEEE Global Communications Conference, GLOBECOM 2020 - Proceedings*, vol. 2020-Janua, 2020, doi: 10.1109/GLOBECOM42002.2020.9348244.
- [29] O. Ibitoye, O. Shafiq, and A. Matrawy, "Analyzing adversarial attacks against deep learning for intrusion detection in IoT networks," *2019 IEEE Global Communications Conference, GLOBECOM 2019 - Proceedings*, 2019, doi: 10.1109/GLOBECOM38437.2019.9014337.

## BIOGRAPHIES OF AUTHORS






**Juli Rejito**    received B.Sc. degree in Mathematics from University of Padjadjaran, Indonesia in 1991, M.Kom. and Dr. in Computer Science from Gadjah Mada University, Indonesia in 2005 and 2014. Currently, he is an Assistant Professor at Dept. of Computer Science, Universitas Padjadjaran, Indonesia. His research interests include Data Science, Artificial Intelligent, Business Intelligent, Data Analytics, Database Systems, Image Processing, Information System, and Machine Learning. He can be contacted at email: juli.rejito@unpad.ac.id.






**Deris Stiawan**    received a Ph.D. degree in Computer Engineering from Universiti Teknologi Malaysia, Malaysia. He is currently a Professor at the Department of Computer Engineering, Faculty of Computer Science, Universitas Sriwijaya. His research interests include computer networks, intrusion detection/prevention systems, heterogeneous networks, and intelligent systems. He can be contacted at email: deris@unsri.ac.id.



**Ahmed Alshafut**    received his M.Sc in Information Technology from Edinburgh Napier University, UK in 2012 and a PhD in Computer Science from King Abdulaziz University in 2019. He is currently an Assistant Professor at the Department of Information Technology, College of Computer and Information, Al-Baha University, Saudi Arabia. His interests are focused on system's administration, data traffic management, new wireless technologies and using technology for assisted living applications. He can be contacted at email: a.alshafut@bu.edu.sa.



**Rahmat Budiarto**    received B.Sc. degree in Mathematics from Bandung Institute of Technology, Indonesia in 1986, M.Eng. and Dr.Eng. in Computer Science from Nagoya Institute of Technology, Japan in 1995 and 1998, respectively. Currently, he is a full professor at Dept. of Computer Science, College of Computer and Information, Albaha University, KSA. His research interests include intelligent systems, brain modeling, IPv6, network security, Wireless sensor networks, and MANETs. He can be contacted at email: rahmat@bu.edu.sa.